UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	No.: 16-cr-10305-NMG
	)	
MARTIN GOTTESFELD,	)	
	)	
Defendant.	)	

GOVERNMENT'S OPPOSITION
TO DEFENDANT GOTTESFELD'S MOTION TO SUPPRESS EVIDENCE

The United States of America, by Assistant United States Attorneys David J. D'Addio and Adam J. Bookbinder, hereby submits this response in opposition to Defendant Martin Gottesfeld's Motion to Suppress Evidence (Dkt. No. 78).

I. INTRODUCTION

Defendant Gottesfeld seeks to suppress evidence obtained from execution of a search warrant at his Somerville apartment on October 1, 2014. He challenges the warrant on two grounds: (1) first, he claims that information obtained from a court-authorized pen register and trap and trace was essential to the probable cause showing and was obtained in violation of the Fourth Amendment and various statutes; (2) second, he claims that the warrant was not sufficiently particular. Both claims are without merit.

As set forth below, the government obtained a Court order to install a pen register and trap and trace ("PRTT") device on the internet service account for the defendant's former residence on July 17, 2014. The PRTT collected non-content routing information—specifically dates, times, IP addresses, and communication ports—for internet activity to and from the internet account servicing that address—28 Albion Street, Apartment 1 in Somerville, Mass.

The court's order and the execution of that order by law enforcement complied fully with the authorizing statute, 18 U.S.C. § 3121-27 (the "Pen/Trap Act"). Defendant nonetheless contends that collecting the specific information authorized by both the Pen/Trap Act and the court order violated his Fourth Amendment rights—a conclusion rejected by every federal court to consider the question, including the Eight Circuit and, this spring, the Second Circuit. The reasoning of these of decisions—unchallenged by the defendant in any meaningful way—is persuasive, is grounded in long-standing Supreme Court precedent, and should be adopted by this Court. Even if this Court were to be the first in the nation to declare the Pen/Trap Act unconstitutional, however, the evidence still should not be suppressed because law enforcement acted reasonably and in good faith when it relied on the Pen/Trap Act and the court's order authorizing installation of a PRTT device to obtain the non-content routing information at issue. Suppression of evidence—a remedy of last resort under the Fourth Amendment—is inappropriate under these circumstances. Moreover, even without the PRTT data, the search warrant affidavit still established probable cause to search the defendant's apartment.

As to the warrant's particularity, the supporting affidavit set forth probable cause to believe that the specific location, and the electronic devices in that location, would constitute or contain evidence of violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 and the federal conspiracy statute, 18 U.S.C. § 371. The attachments to the warrant set forth these statutory violations and further provided specific examples of the types of documents and information to be seized. In short, there are no grounds to suppress the evidence obtained from the October 1, 2014 search. For these reasons, defendant's motion should be denied.

II. BACKGROUND

A. The Pen/Trap Act Authorizes Prospective Collection of Addressing and Routing Information, Such as IP Addresses, for 60 Days.

The Pen/Trap Act authorizes installation of a "pen register" to record or capture, prospectively, "dialing, routing, addressing, or signaling information" that is "transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). The Pen/Trap Act prohibits collection of "the contents of any communication," *id.*, thus drawing a distinction between the non-content information necessary to route a communication from its source to its destination, and the content of the communication itself.

Similarly, the Pen-Trap Act authorizes installation of a "trap and trace" device to "identify the originating number or . . . source of a wire or electronic communication," 18 U.S.C. § 3127(4). Like the pen register provision, the trap and trace provision prohibits collection of "the contents of any communication." *Id.* To install either device, the government must certify that the information likely to be collected is "relevant to an ongoing criminal investigation" but it is not required to establish probable cause or obtain a warrant. 18 U.S.C. § 3122.

Congress amended the Pen/Trap Act in 2001 explicitly to include non-content addressing information for internet communications, in addition to telephone toll records. USA Patriot Act, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288 (2001); 147 Cong. Rec. S11,006 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) (describing amendment as a way to "ensure[ ] that the pen register and trap and trace provisions apply to facilities other than telephone lines (e.g., the Internet)"); 147 Cong. Rec. S11,049 (daily ed. Oct. 25, 2001) (statement of Sen. Kyl) (noting that language ultimately adopted "would codify current case law that holds that pen/trap orders apply to modern communication technologies such as e-mail and the Internet, in addition to traditional phone lines."); 147 Cong. Rec. H7,197 (daily ed. Oct. 23, 2001) (statement of Rep.

Conyers) (describing amendment as extending "the pen/trap provisions so they apply not just to telephone communications but also to Internet traffic, so long as they exclude 'content.'"). *See generally In the Matter of Application of the United States of America for an Order Authorizing the Installation and Use of A Pen Register and a Trap & Trace Device on E-Mail Account*, 416 F. Supp. 2d 13, 16-17 (D.D.C 2006) (discussing text and legislative history of Pen/Trap Act and concluding: "The plain language of the statute makes clear that pen registers and trap and trace devices may be processes used to obtain [routing] information about e-mail communications. The statute's history confirms this interpretation and there is no support for a contrary result.")

B. <u>The Government Obtained Authorization to Install a PRTT Device to Capture Source and Destination IP Addresses For Internet Traffic Over Defendant's Internet Service Account.</u>

On July 17, 2014, the government applied for an order seeking authorization under the Pen/Trap Act to install, for 60 days, a pen register and trap and trace device "to trace the source and destination of all electronic communication directed to or originating from" the RCN Telecom Services LLC ("RCN") account providing internet service to 28 Albion Street, Apt. 1, in Somerville—the Defendant's prior address—along with the date, time, size, and duration of these communications. Dkt. No 78, Ex. C at 4. The application expressly stated the "United States does not seek 'content,' in any form, of any electronic communication." The application further provided that the government "does not seek the URL for websites visited by the designated account, as this URL could contain content." *Id.* Regarding the types of non-content routing information at issue, the application explained:

> Data packets transmitted over the internet—the mechanisms for all internet communications—contain addressing and routing information analogous to the destination phone numbers captured by traditional pen registers and the origination phone numbers captured by traditional trap and trace devices. One example of this addressing and routing information is an IP address, which is a unique numeric address used by computers on the internet. Another example of this addressing and routing information is a "port,"

> which is a numeric identifier of a particular type of service being offered by a computer or server. For example, port 80 is typically reserved for World Wide Web traffic, so that a computer that wishes to retrieve information from a web server would typically connect to port 80.

Id. at 2.

On July 17, 2014, U.S. Magistrate Judge Jennifer C. Boal issued an order authorizing law enforcement to install a pen register/trap and trace device to capture, for 60 days, "the source and destination IP address and port of all electronic communications," along with the date and time of those communications, to or from the defendant's internet service account with RCN.[1] Dkt. No. 78, Ex. C. at 2. An example of the data provided to the FBI via the PRTT device is provided in the table below:

Start Date (UTC)	Source IP	Source Port	Destination IP	Destination Port
8/9/2014 11:48 AM	209.6.193.140	1534	50.57.60.203	161
8/9/2014 11:48 AM	209.6.193.140	1536	50.57.60.203	161
8/9/2014 11:47 AM	209.6.193.140	1541	50.57.60.203	161

RCN provided no additional types of information (*e.g.*, file size, duration of communication, or any manner of content). The government produced the data provided by RCN to defense counsel in discovery.

C. <u>The Government Obtained a Warrant to Search Defendant's Residence.</u>

On September 30, 2014, the Honorable Marianne B. Bowler issued a warrant to search defendant's residence, at 28 Albion Street, Apartment 1, in Somerville, Mass. The warrant application incorporated a supporting affidavit that described the distributed denial of service perpetrated against the computer network of the Boston Children's Hospital, along with an array of evidence linking Gottesfeld to that cyberattack as well as attacks on other entities Gottesfeld

[1] The order further authorized collection of the "size" of the communications and their duration—neither of which constitutes the content of the communications. However, this information was not provided by RCN.

campaigned against. The warrant authorized agents to search for and seize evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030(a)(5)(A) (intentionally causing damage to a protected computer) and 18 U.S.C. § 371 (conspiracy). More specifically, the warrant set forth a list enumerating, among other things, specific people, entities, IP addresses, websites, social media accounts, and topics relating to the Children's Hospital DDOS attack and other entities targeted by Gottesfeld and/or the hacking collective known as "Anonymous," for which the warrant authorized the search. Agents executed the warrant on October 1, 2014, seizing multiple electronic devices containing evidence of Gottesfeld's involvement in the attack on the Boston Children's Hospital.

After the search, Gottesfeld retained counsel and began discussions with the U.S. Attorney's Office about a possible pre-indictment plea. But on February 16, 2016, after the government learned that Gottesfeld and his wife had fled the country in a small boat, the U.S. Attorney charged him, by criminal complaint, with conspiracy (18 U.S.C. § 371) to intentionally cause damage to protected computers (18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B)). Gottesfeld was arrested in Miami on February 17, 2016. He was indicted, on October 19, 2016, on one count each of conspiracy and damaging protected computers.

III. ARGUMENT

A. Collection of IP Addresses Is Not a Search Under the Fourth Amendment

The Supreme Court has held, in the context of telephones, that the use of a pen register does not constitute a "search" under the Fourth Amendment, for which a warrant is required, because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," such as the dialing instructions he conveys to telephone companies when he makes a call. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). *See also United States v. Miller*, 425 U.S. 435 (1976) (no expectation of privacy in information voluntarily turned over to

banks as reflected in banking records). This same principle behind the "third party doctrine" applies when a pen register is used to collect data, such as IP addresses, that is used to route electronic communications over the internet—a circumstance that is "constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*." *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008).

Just like telephone users, internet users "rely on third-party equipment in order to engage in communication" and "have no expectation of privacy in . . . the IP addresses of the websites they visit, because they should know that this information is provided to and used by internet service providers for the specific purpose of directing the routing of information." *Forrester*, 512 F.3d at 510; *accord United States v. Ulbricht*, 858 F.3d 71, 96 (2d Cir. 2017). Indeed, "IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over to direct the third party's servers." *Ulbricht*, 858 F.3d at 96 (quoting *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010)).

Earlier this year, in *Ulbricht*, the Second Circuit squarely rejected a Fourth Amendment challenge to the Pen/Trap Act that mirrored that brought by defendant Gottesfeld. *Ulbricht*, 858 F.3d at 96. Addressing the collection of the same IP routing information at issue here, the Second Circuit concluded:

> The recording of IP address information and similar routing data, which reveal the existence of connections between communications devices without disclosing the content of the communications, are precisely analogous to the capture of telephone numbers at issue in *Smith*. . . . The substitution of electronic methods of communication for telephone calls does not alone create a reasonable expectation of privacy in the identities of devices with whom one communicates. Nor does it raise novel issues distinct from those long since resolved in the context of telephone communication, with which society has lived for the nearly forty years since *Smith* was decided. Like telephone companies, Internet service providers require that identifying information be disclosed in order to make

> communication among electronic devices possible. In light of the *Smith* rule, no reasonable person could maintain a privacy interest in that sort of information.

Ulbricht, 858 F.3d at 97.

Accordingly, IP addresses and similar internet routing information are not protected by the Fourth Amendment and can be collected without a warrant under the Pen/Trap Act. *See Ulbricht*, 858 F.3d at 97 (joining other circuits and holding that "collecting IP address information devoid of content is 'constitutionally indistinguishable'" from the use of a telephone pen register) (quoting *Forrester*, 512 F.3d at 510). *See also United States v. Graham*, 824 F.3d 421, 432 (4th Cir. 2016) (en banc) (noting that "third-party information relating to the sending and routing of electronic communications does not receive Fourth Amendment protection"); *United States v. Carpenter*, 819 F.3d 880, 887 (6th Cir. 2016) ("[C]ourts have not (yet at least) extended [Fourth Amendment] protections to the internet analogue of envelope markings, namely the metadata used to route internet communications like . . . IP addresses"). *See generally In the Matter of Application of the United States of America for an Order Authorizing the Installation and Use of A Pen Register and a Trap & Trace Device on E-Mail Account*, 416 F. Supp. 2d 13, 16-17 (D.D.C 2006) (applying Pen/Trap Act to email accounts where government "explicitly identif[ied] the information" the PRTT was to collect and omitted "content" of the communications); *In re Application of U.S. for an Order Authorizing use of A Pen Register & Trap On (XXX) Internet Serv. Account/User Name, (xxxxxxxx@xxx.com)*, 396 F. Supp. 2d 45, 48 (D. Mass. 2005) (Collings, J.) (finding with regard to an internet PRTT application that: "If, indeed, the government is seeking only IP addresses of the web sites visited and nothing more, there is no problem").

Recognizing that the third-party doctrine is fatal to his claim, defendant invites this Court to disregard it, arguing that the third-party doctrine is "at odds with the pervasive use of technology today" and noting that the "Supreme Court is poised to revisit the third party doctrine," which the Defendant concedes has "heretofore insulated this information from Fourth Amendment protection." Dkt. No. 78 at 4. Defendant argues that if he is liberated from this precedent, then IP addresses for his internet activity, when aggregated over the 60-day period authorized by the Pen/Trap Act, constitute information in which he has a reasonable expectation of privacy under *Katz v United States*, 389 U.S. 437 (1967). Dkt. 78 at 5-6. In the alternative, he claims that IP addresses themselves constitute the *content of his communications*, and therefore obtaining such routing information without a warrant violated the Fourth Amendment, as well as the Pen/Trap Act and the Wiretap Act, 18 U.S.C. §§ 2510-22. As is discussed below, these arguments are meritless.

B. <u>Defendant Has No Reasonable Expectation of Privacy in Routing Data Obtained Under the Pen/Trap Act.</u>

The Fourth Amendment's prohibition on unreasonable searches was originally understood to be "tied to common-law trespass." *United States v. Jones*, 565 U.S. 400, 405 (2012). Since the Supreme Court's decision in *Katz*, however, a Fourth Amendment search may also "occur[] when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo* v. *United States*, 533 U.S. 27, 33 (2001). The First Circuit has accordingly stated, "The Supreme Court set out a two-part test for analyzing the expectation [of privacy] question: first, whether the movant has exhibited an actual, subjective, expectation of privacy; and second, whether such subjective expectation [of privacy] is one that society is prepared to recognize as objectively reasonable." *United States v. Rheault*, 561 F.3d 55, 59 (1st Cir. 2009) (citing *Smith*, 442 U.S. at 740).

i. Defendant Has Failed To Assert a Subjective Expectation of Privacy in the Source and Destination IP Addresses of his Internet Communications.

Establishing a reasonable expectation of privacy is the defendant's burden. *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980); *United States v. Lewis*, 40 F.3d 1325, 1333 (1st Cir. 1994). When a defendant fails to provide an affidavit in support of a motion to suppress, "it is almost impossible to find a privacy interest because this interest depends, in part, on the defendant's subjective intent and his actions that manifest that intent." *United States v. Ruth*, 65 F.3d 599, 604-05 (7th Cir. 1995). Here, Defendant has failed to file an affidavit in support of his motion, which rests only on the limited, conclusory statements of his lawyers regarding his expectation of privacy in his own IP address and those of the servers with which he communicated via the internet. The only suggestion that the defendant actually believed that the routing information for his internet activity was private is his lawyers' assertion that the defendant "used encryption services—the only way an individual can attempt to hold onto his privacy while using the internet." Dkt. No. 78 at 7. Far from establishing a subjective expectation of privacy, defendant's use of anonymizing technologies suggests the opposite—that he knew that routing information regarding his internet traffic was not private, but instead was available to his internet service provider and servers he communicated with, as this information must be conveyed in order for internet traffic to flow. Thus, he used various encryption services to attempt to limit his public exposure. Because the defendant has failed to assert a subjective privacy interest in the routing information at issue, the Court may deny the defendant's motion to suppress without a hearing. *See United States v. Lewis*, 40 F.3d 1325, 1333 (1st Cir. 1994).

ii. Any Subjective Expectation of Privacy in IP Routing Information Is Objectively Unreasonable.

Even if Defendant were to establish that he personally expected the non-content routing information for his internet traffic would be private, such an expectation is not one that society

recognizes as reasonable. "Like telephone companies, Internet service providers require that identifying information be disclosed in order to make communication among electronic devices possible. In light of the *Smith* rule, no reasonable person could maintain a privacy interest in that sort of information." *Ulbricht*, 858 F.3d at 97. This basic proposition, built upon binding Supreme Court precedent, is further buttressed in this case by Congress's decision to expressly incorporate the *Smith* rule when it expanded the Pen/Trap Act to cover internet communications. *See supra* Part II.A.[2] Although this defendant claims that real-time collection of internet routing information, "for 60 days, goes well beyond what ordinary people expect the government to be observing," Dkt. No. 78, that this is precisely what the "ordinary people's" elected representatives authorized the government to collect in passing the 2001 amendments to the Pen/Trap Act.[3]

Defendant recognizes that the "third-party doctrine" has to date precluded any Fourth Amendment claim where the government compels disclosure of records voluntarily provided to a third party, including the records for routing internet traffic at issue here. Dkt. No. 78 at 8. He nonetheless contends that the third-party doctrine is inconsistent with the widespread use of modern technology, relying principally on Justice Sotomayor's concurrence in *Jones*, 565 U.S. at 414 and the majority opinion in *Riley v. California*, 134 S. Ct. 2473 (2014). Dkt. No. 78 at 8-9. He further notes that some states have limited the application of the third-party doctrine to

[2] As the House of Representatives noted in its report regarding the enactment of the PATRIOT Act, "the statutorily prescribed line between a communication's contents and non-content information" is "identical to the constitutional distinction drawn by the U.S. Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 741–43 (1979)." H.R. Rep. No. 107–236, at 53 (Oct. 11, 2011).

[3] This point is a crucial one and distinguishes the instant case from *Jones*, in which law enforcement used GPS devices to track the suspect's precise location for 28 days, 565 U.S. at 402-03, without any express authorization by a court or Congress.

certain technologies under state law, and that the Supreme Court is "poised to reconsider the third party doctrine this coming term." *Id*. at 8, 10.

Whatever the Supreme Court might decide in the future with respect to the third-party doctrine, this Court remains bound by the holdings of *Smith* and *Miller* unless and until the Supreme Court overrules them. *See United States v. Ivery*, 427 F.3d 69, 75 (1st Cir. 2005) ("It is not our place to anticipate the Supreme Court's reconsideration of its prior rulings"). Indeed, the Supreme Court "has admonished the lower federal courts to follow its directly applicable precedent, even if that precedent appears weakened by pronouncements in its subsequent decisions, and to leave to the [Supreme] Court 'the prerogative of overruling its own decisions.'" *Figueroa v. Rivera*, 147 F.3d 77, 81 n.3 (1st Cir. 1998) (quoting *Agostini v. Felton*, 521 U.S. 203, 237 (1997). *See also Ulbricht*, 858 F.3d at 96-97 (rejecting Ulbricht's call to re-evaluate the *Smith* doctrine in light of "great quantities of personal information" provided to third parties).

In any event, Defendant's reliance on *Jones* and *Riley* to sidestep the third-party doctrine is misplaced. *Jones* and *Riley* did not address—much less disavow—the Supreme Court's precedents recognizing that an individual does not have a Fourth Amendment interest in a third party's records pertaining to him or in information that he voluntarily conveys to third parties. Because the Court in *Jones* concluded that the attachment of a GPS device constituted "a classic trespassory search," 565 U.S. at 412, it did not reach the *Katz* inquiry.[4] *Riley* is even further afield. *Riley* held that a law-enforcement officer generally must obtain a warrant to search the

[4] Defendant cites *dicta* addressing *Katz* in a wholly distinct context: aggregation of 28 days of data obtained from law enforcement's covert installation and use of GPS tracking device without a warrant, court order, or any express statutory authorization. Here, in contrast, the government used compulsory process in the form of a court order expressly authorized by statute to obtain records of information the defendant' voluntarily turned over to a third party—his internet service provider.

contents of a cell phone found on an arrestee. 134 S. Ct. at 2485. No question existed in *Riley* that the review of the contents of a cell phone constitutes a Fourth Amendment search; the question was whether that search fell within the traditional search-incident-to-arrest exception to the warrant requirement. *See id.* at 2482 ("The two cases before us concern the reasonableness of a warrantless search incident to a lawful arrest."); *see also id.* at 2489 n.1 (noting that "[b]ecause the United States and California agree that these cases involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances"). Neither *Jones* nor *Riley* presented an occasion for the Supreme Court to reconsider its longstanding view that an individual has no Fourth Amendment interest in records pertaining to an individual that are created by third parties or in information he voluntarily conveys to third parties. Nor do these cases provide any grounds for this Court to otherwise distinguish *Smith* and *Miller* in the context of internet routing data.

Likewise, defendant's citations to state law (almost all of which deal with legally distinct concepts and a separate statutory scheme for obtaining historical cell phone location data) are misplaced. The Supreme Court has repeatedly rejected the "suggestion that concepts of privacy under the law of each State are to determine the reach of the Fourth Amendment." *California v. Greenwood*, 486 U.S. 35, 44 (1988). Rather, "when States go above the Fourth Amendment minimum, the Constitution's protections concerning search and seizure remain the same." *Virginia v. Moore*, 553 U.S. 164, 173 (2008). In any case, the enactment of state laws addressing business records such as cell site location records and pen register data confirms that legislatures are best positioned to balance privacy interests and law enforcement needs in light of new

technologies, just as Congress has already done with the Pen/Trap Act. *See Jones*, 565 U.S. at 429-30 (Alito, J. concurring in the judgment).

In short, *Smith* and *Miller* remain controlling law; Congress adopted a statute incorporating those holdings and expressly authorizing law enforcement to collect the internet routing data at issue in this case; and agents followed the statutory procedure in obtaining and executing a court order to collect that information. *See Ulbricht* 858 F.3d at 96-97; *Forrester* 512 F.3d at 510. Accordingly, no Fourth Amendment search occurred, and defendant's motion should be denied.

C. The Internet Routing Information Collected by the Government Is Not "Content."

Defendant "contends that continuous tracking of his online activities, in real time, 24 hours a day for 60 days, garners information that constitutes 'content,'" Dkt. No. 78 at 11, and that accordingly, acquisition of IP addresses via the PRTT violated not only the PRTT, but the Wiretap Act and the Fourth Amendment.

Defendant's argument falters at the first step. As discussed in Part II.A, *supra*, the Pen/Trap Act authorizes collection of "dialing, routing, addressing, or signaling information," but prohibits collection of "the contents of any communication." There is no question that the "dialing, routing, address, or signaling information" includes source and destination IP addresses for internet communications. *See* Part II.A, *supra*. By defining aggregated IP addresses as "content," defendant renders the Pen/Trap Act a nullity for the very types of communications it was intended to cover—*i.e.*, the Pen/Trap Act cannot authorize the collection of IP addresses while *simultaneously prohibiting* the collection of those same IP addresses. Such a reading of the Pen/Trap Act is nonsensical, is untethered from any authority cited by the defendant, and should be rejected out of hand by this Court.

Defendant goes on, however, to offer hypothetical circumstances in which information that might be considered routing information, may also convey the "the substance, purport, or meaning of that communication," 18 U.S.C. § 2510(8), and thus constitute "content" within the meaning of the Pen/Trap Act, 18 U.S.C. § 3127(1) and the Wiretap Act. Oft-cited examples include, in the context of telephone calls, so-called "post-cut-through digits," (*i.e.*, numbers dialed after the initial call is placed or "cut through"), and in the context of internet traffic, website Uniform Resource Locators ("URLs") that can contain information such as search terms entered or specific web pages visited. *See generally, In re Google, Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 128, 135-39 (3d Cir. 2015); *In re Application of U.S. for an Order Authorizing use of A Pen Register & Trap On (XXX) Internet Serv. Account/User Name, (xxxxxxxx@xxx.com)*, 396 F. Supp. 2d 45, 47-69 (D. Mass. 2005) (Collings, J.).

None of these concerns are present in this case, where the routing information consisted solely of IP addresses, communication ports, dates, and times. Just as no court has ever held that the initial telephone number dialed (or incoming number received) constitutes the "contents" of a telephone communication, no court has ever held that an incoming or outgoing IP address constitutes the "contents" of an electronic communication made via the internet. Every relevant case cited by the defendant either holds or assumes the same. The Court therefore stands on firm ground in rejecting the claim actually made by the defendant—that IP addresses can constitute communicative content as opposed to routing information—and deferring judgment on his discussion regarding when other types of routing information not relevant to this case may simultaneously constitute communicative "content." *See Ulbricht*, 858 F.3d at 98 n.29 (confining its opinion to "the capture of IP addressed, TCP connection data, and similar routing information" under the Pen/Trap Act), *Forrester*, 512 F.3d at 510-11, 511 n.6 (noting that

surveillance techniques that collect URLs "might be more constitutionally problematic" and limiting its holding to IP addresses and email to/from addresses).

Defendant's claim that the government "has obtained a layer of information beyond simply the IP addresses with whom Gottesfeld communicated" is wrong. The government produced to defendant the PRTT data—it consists solely of dates, times, source and destination IP addresses, and source and destination ports. Defendant is correct that the warrant application states the affiant's belief, based on those IP addresses, that the defendant used the VPN network riseup.net, and the TOR network. As defendant well knows, however, the registration of IP addresses is a matter of public record, and TOR network nodes are also publicly listed. Just as a PRTT on a phone reveals dialed numbers that law enforcement can look up, a PRTT on an internet account reveals IP addresses that law enforcement can look up. In this case, a simple internet query reveals that certain IP addresses with which defendant communicated belonged to particular internet services, including Riseup.net and TOR.

Finally, defendant quibbles with the form of the court's PRTT order, claiming it was inadequate because it did not offer what the defendant believes were sufficient assurances that RCN would not provide information outside the scope of the statutory authorization. Dkt. No.78 at 12-13. The proper measure of the Order, however, is the statute under which it was promulgated, not the defendant's view of best practices. The Order clearly stated that the PRTT device was to provide the "source and destination IP address and port of all electronic communications directed to or originating from the designated account, and to record the date, time, size, and duration of these communications. . . . *RCN shall not provide to the FBI, the URL for websites visited by the designated account*." Dkt. No. 78, Ex. C at 2 (emphasis added). In short, the court ordered RCN to provide limited, specifically enumerated categories of

information authorized by the statute, and expressly instructed RCN not to provide URLs that, although used for routing, could constitute "content" in certain circumstances. Most important, RCN in fact provided only the dates, times, and source and destination IP addresses and ports—nothing more. There is simply no information RCN provided that could constitute content under any definition in the relevant statutes or case law, and defendant, despite having the actual data, has pointed to none.

D. Law Enforcement Was Entitled To Rely On A Presumptively Constitutional Statute and a Duly Executed Order of the Court in Obtaining the Routing Information at Issue.

The exclusionary rule is a "judicially created remedy" that is "designed to deter police misconduct rather than to punish the errors of judges and magistrates." *United States v. Leon*, 468 U.S. 897, 906, 916 (1984). "As with any remedial device, application of the exclusionary rule properly has been restricted to those situations in which its remedial purpose is effectively advanced." *Illinois v. Krull*, 480 U.S. 340, 347 (1987). The rule therefore does not apply "where [an] officer's conduct is objectively reasonable" because suppression "cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity." *Leon*, 468 U.S. at 919. For that reason, "evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *Id.* (citation omitted).

This good-faith exception applies to "officer[s] acting in objectively reasonable reliance on a statute," later deemed unconstitutional, that authorizes warrantless administrative searches. *Krull*, 480 U.S. at 349. It follows *a fortiori* that officers act reasonably in relying on a statute that authorizes the acquisition of records only pursuant to an order issued by a neutral magistrate. The Supreme Court has explained:

> The application of the exclusionary rule to suppress evidence obtained by an officer acting in objectively reasonable reliance on a statute would have as little deterrent effect on the officer's actions as would the exclusion of evidence when an officer acts in objectively reasonable reliance on a warrant. *Unless a statute is clearly unconstitutional, an officer cannot be expected to question the judgment of the legislature that passed the law*. If the statute is subsequently declared unconstitutional, excluding evidence obtained pursuant to it prior to such a judicial declaration will not deter future Fourth Amendment violations by an officer who has simply fulfilled his responsibility to enforce the statute as written. To paraphrase the Court's comment in *Leon*: *"Penalizing the officer for the [legislature's] error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations."*

Krull, 480 U.S. at 349-50 (emphasis added).

Thus, even if the Court were to become the first to declare the Pen/Trap Act unconstitutional as applied to IP addresses, law enforcement was nonetheless entitled to rely on the strong presumption that statutes are constitutional. *See United States* v. *Watson*, 423 U.S. 411, 416 (1976) (applying a "strong presumption of constitutionality" when assessing challenges to a federal statute under the Fourth Amendment) (citation omitted). At the time the PRTT device was installed in this case, moreover, no binding appellate decision (or holding of any circuit) had suggested, much less held, that the Pen/Trap Act was unconstitutional as applied to internet routing information such as IP addresses. As discussed above, all federal authority was, and remains, to the contrary. Under such circumstances, "an officer cannot be expected to question the judgment of the legislature that passed the law" and therefore suppression "cannot logically contribute to the deterrence of Fourth Amendment violations." *Krull*, 480 U.S. at 349-50. *Cf. Davis v. United States*, 564 U.S. 229, 241 (2011) ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule"). *See also, United States v. Russell Rose*, 914 F. Supp. 2d 15, 22-24 (D. Mass. 2012) (Gorton, J.) (applying *Davis* to deny motion to suppress warrantless GPS tracking evidence where officers

reasonably relied on non-binding precedent). Such reliance is all the more reasonable when law enforcement sought and obtained a court order from a neutral magistrate. Under such circumstances, suppression would serve no Constitutional interest.

E. The Government Complied With All Aspects of the Pen/Trap Act, the Stored Communications Act, and the Wiretap Act.

Gottesfeld claims that the installation of the PRTT in this case violated the Stored Communications Act ("SCA"), 18 U.S.C. § 2703. Dkt. #78 at 14. The SCA, however, is irrelevant to the installation and monitoring of the PRTT device. As described in Part II.A, *supra*, the Pen/Trap Act authorizes the installation of a PRTT device upon the government's certification that the information is "relevant to an ongoing criminal investigation." 18 U.S.C. § 3122. No recitation of facts is required. Defendant simply conflates the two statutes, and the two separate standards they set forth for obtaining different types of information.

Because the defendant has not established a single instance in which "content" of his communications was obtained by the government, see Part II.C, *supra*, his claim that the PRTT violated the Wiretap Act must also fail.[5]

F. The Search Warrant Affidavit Established Probable Cause to Search Defendant's Residence Even Without the Pen Trap Data.

Even if the Court were, as Gottesfeld urges, to excise from the search warrant affidavit the results of the PRTT, the affidavit nonetheless established probable cause to search Gottesfeld's residence. In determining whether the excised affidavit established probable cause,

[5] The government notes further that defendant has not engaged the text of the Wiretap Act, nor the substantial body of case law devoted to interpreting the interception of electronic communications. "Few principles are more sacrosanct in this circuit than the principle that 'issues averted to in a perfunctory manner, unaccompanied by some effort at developed argumentation, are deemed waived.'" *Redondo-Borges v. U.S. Dep't of Hous. & Urban Dev.*, 421 F.3d 1, 6 (1st Cir. 2005) (quoting *United States v. Zannino*, 895 F.2d 1, 17 (1st Cir.1990)). This principal alone dooms his argument that the government's collection of IP addresses violated the Wiretap Act.

the question is whether a person of "reasonable caution" would believe that evidence of a crime would be found based on the affidavit included with the warrant. *United States v. Woodbury*, 511 F.3d 93, 98 (1st Cir. 2007).

Gottesfeld concedes that the affidavit established that he posted the YouTube video calling for action against Children's Hospital if it did not fire a particular doctor and discharge the teenage patient back to her family. Dkt. 78 at 16; Dkt. 78 Ex. 1, ¶¶ 16-18. More specifically, the affidavit establishes that, not only did Gottesfeld's YouTube account post the YouTube video, that video was posted from the IP address assigned to Gottesfeld's residence, meaning that someone at that residence "used a computer, tablet, smartphone, or other internet-enabled device" to post the video. *Id.* ¶¶ 16-18.

The affidavit also described that the video that Gottesfeld posted included a link to a posting, on the website pastebin.com, that listed detailed information about Children's Hospital's web server, including its IP address and server type. Dkt. 78 Ex. 1 ¶¶ 10-14. This is the server that was later attacked. When the hospital did not meet the demands set out in the video, the server identified in the pastebin.com posting was subjected to a distributed denial of service (DDOS) attack, which caused significant disruption to the hospital website and computer network. *Id.* ¶¶ 6-8.

The affidavit also described connections between Gottesfeld and other DDOS attacks against entities associated with what Gottesfeld called the "troubled teen industry." The affidavit described how Gottesfeld targeted a treatment center in Utah via social media accounts. *Id.*[6] ¶¶ 29-30. That treatment center then experienced a DDOS attack, as did the company that

[6] While they are included in the affidavit, which was filed under seal, the government has not publicly disclosed the names of these additional DDOS victims.

provided its records management. *Id.* ¶ 29. And the affidavit describes how Gottesfeld threatened to add a school-listing website to his campaign against the Utah treatment center if the website did not remove the center from its listings. *Id.* ¶ 31. That website, too, later suffered a DDOS attack. *Id.*

While these links to other DDOS attacks provide additional support for the probable cause finding, it is the direct connection between Gottesfeld's YouTube account and home IP address and the video threatening Children's Hospital (and the linked pastebin posting) that most directly establishes probable cause for the search. The threat and the linked pastebin posting, providing targeting information, are critical pieces of evidence of the crimes under investigation – not just the crime of damaging a computer (18 U.S.C. § 1030) but also the conspiracy among those responsible for threatening, organizing, and orchestrating this attack (18 U.S.C. § 371). *Id.* ¶ 2. By establishing that Gottesfeld's YouTube account posted the video from an internet-connected device at Gottesfeld's residence, the affidavit established probable cause to search that residence for that device and for other evidence and instrumentalities of these crimes.

G. <u>The Search Warrant Was Sufficiently Particular.</u>

In arguing that the search warrant was unconstitutionally overbroad, Gottesfeld misreads both the affidavit and the case law.

The Fourth Amendment requires that warrants particularly describe "the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The warrant in this case fulfilled this requirement. Attachment A to the warrant described in detail Gottesfeld's residence and included a photo. Dkt. 78 Attachment A. Attachment B to the warrant described in great detail the kinds of evidence to be seized. Dkt. 78 Attachment B. Specifically, section I of that attachment lists a series of people, entities, IP addresses, accounts, topics, location and identity information, and computer-specific evidence relevant to the crimes being investigated.

In support of his overbreadth claim, Gottesfeld focuses on the first sentence of section II of Attachment B, which authorizes the seizure of "[a]ll computer hardware (including smartphones and tablets), computer software, and storage media." Dkt. 78 at 17, Attachment B. But he neglects to mention the second sentence of that section, which states: "Off-site searching of these items shall be limited to searching for the items described in paragraph I." Nor does he mention that the affidavit describes in great detail, in paragraphs 34(a)-(b), why off-site searching of electronic devices is often necessary. Finally, while Gottesfeld criticizes the language in Affidavit paragraph 35 seeking permission to search and seize items "regardless of how their contents or ownership appear or are described by others at the scene of the search," he neglects to mention that the first three sentences of paragraph 35 explain why this is appropriate:

> The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant.

Dkt. 78 Exhibit 1 ¶ 35.

Gottesfeld bases his legal argument on the recent decision in *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017), but that case is distinguishable in many was from the situation presented here. In *Griffith*, police obtained a warrant to search the defendant's apartment in connection with their investigation of a homicide. *Id.* at 1268. The affidavit outlined evidence suggesting that Griffith was involved in the homicide and now lived in the apartment with his girlfriend. *Id*. at 1269. The affiant then relied on his training and experience and that of other officers to conclude that gang members maintain regular contact with each other and "often stay advised and share intelligence about their activities through cell phones and other electronic communication devices and the Internet, to include Facebook, Twitter and E-mail accounts." *Id.*

The affidavit then concluded: "Based upon the aforementioned facts and circumstances, and your affiant's experience and training, there is probable cause to believe that secreted inside of [the apartment] is evidence relating to the homicide discussed above." *Id.* In light of the paucity of the affidavit, the court, in *Griffith*, held:

> the affidavit supporting the warrant application provided virtually no reason to suspect that Griffith in fact owned a cell phone, let alone that any phone belonging to him and containing incriminating information would be found in the residence. At the same time, the warrant authorized the wholesale seizure of all electronic devices discovered in the apartment, including items owned by third parties. In those circumstances, we conclude that the warrant was unsupported by probable cause and unduly broad in its reach.

Id. at 1270-71.

The Gottesfeld affidavit could not have been more different from that in *Griffith*. It established that, not only did Gottesfeld's YouTube account post the YouTube video, that video was posted from the IP address assigned to Gottesfeld's residence, meaning that someone at that residence "used a computer, tablet, smartphone, or other internet-enabled device" to post the video. Dkt. 78 Ex. 1, ¶¶ 16-18. It also described how the PRTT records demonstrated that internet traffic from Gottesfeld's residence was using two anonymizing tools that were also being used by two Twitter accounts that were tweeting at or about the DDOS victims during and after the attacks. *Id.* ¶¶ 21-26. This affidavit, therefore, unlike that in *Griffith*, established probable cause that there were internet-capable devices in Gottesfeld's residence, that one or more of them would contain relevant evidence, and that it might not be possible to determine at the scene which device contained the relevant evidence. *Id.* ¶¶ 16-18, 21-26, 35.[7] The warrant in this case was, therefore, not unconstitutionally overbroad.

[7] *See United States v. McLellan*, 792 F.3d 200, 213 (1st Cir. 2015) (where there was one internet router for a residence, every internet connection established from any of the residence's computers would trace back to the same IP address).

H. Law Enforcement Relied in Good Faith on a Facially Valid Warrant.

Finally, even if this Court deemed the warrant deficient, "it could hardly be called so overbroad (or lacking in probable cause) 'as to render official belief in its [validity] entirely unreasonable.'" *United States v. Jenkins*, 680 F.3d 101, 107 (1st Cir. 2012) (quoting *Leon*, 468 U.S. at 923). This is a far cry from the rare case where a warrant is so clearly insufficient as to merit the "extreme sanction of exclusion[.]" *Leon*, 486 U.S. at 926. *Cf. United States v. Ricciardelli*, 998 F.2d 8, 15 (1st Cir. 1993) (exclusion not proper where existence of probable cause was a "borderline call"); *United States v. Beckett*, 321 F.3d 26, 32-33 (1st Cir. 2003) (exclusion not proper even when evidence of nexus between criminal activity and residence was "less than overwhelming"). Because it cannot "be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment," *Leon*, 468 U.S. at 919, applying the exclusionary rule would not deter future Fourth Amendment violations and therefore is inappropriate in these circumstances, *Krull*, 480 U.S. at 347.

For all of these reasons, the Court should deny Gottesfeld's Motion to Suppress.

Respectfully submitted,

William D. Weinreb
Acting United States Attorney

By: */s/ Adam Bookbinder*
Adam J. Bookbinder
David J. D'Addio
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Adam Bookbinder

Dated: October 6, 2017